WO 01/86601
PCT/FR01/01359

TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

AVIS INFORMANT LE DÉPOSANT DE LA COMMUNICATION DE LA DEMANDE INTERNATIONALE AUX OFFICES DÉSIGNÉS

(règle 47.1.c), première phrase, du PCT)

Destinataire:
CORLU, Bernard
Bull CP8
PC62A24
68, route de Versailles
Boîte postale 45
F-78431 Louveciennes Cedex
FRANCE

Date d'expédition (jour/mois/année) 15 novembre 2001 (15.11.01)		
Référence du dossier du déposant ou du mandataire PCT 3879/BC	AVIS IMPORTANT	
Demande internationale n° PCT/FR01/01359	Date du dépôt international (jour/mois/année) 04 mai 2001 (04.05.01)	Date de priorité (jour/mois/année) 09 mai 2000 (09.05.00)
Déposant BULL CP8 etc		

1. Il est notifié par la présente qu'à la date indiquée ci-dessus comme date d'expédition de cet avis, le Bureau international a **communiqué**, comme le prévoit l'article 20, la demande internationale aux offices désignés suivants:
   KR,US

   Conformément à la règle 47.1.c), troisième phrase, ces offices acceptent le présent avis comme preuve déterminante du fait que la communication de la demande internationale a bien eu lieu à la date d'expédition indiquée plus haut, et le déposant n'est pas tenu de remettre de copie de la demande internationale à l'office ou aux offices désignés.

2. Les offices désignés suivants ont renoncé à l'exigence selon laquelle cette communication doit être effectuée à cette date:
   AU,BR,CA,CN,EP,JP,NO,SG

   La communication sera effectuée seulement sur demande de ces offices. De plus, le déposant n'est pas tenu de remettre de copie de la demande internationale aux offices en question (règle 49.1)a-bis)).

3. Le présent avis est accompagné d'une copie de la demande internationale publiée par le Bureau international le
   15 novembre 2001 (15.11.01) sous le numéro WO 01/86601

RAPPEL CONCERNANT LE CHAPITRE II (article 31.2)a) et règle 54.2)

Si le déposant souhaite reporter l'ouverture de la phase nationale jusqu'à 30 mois (ou plus pour ce qui concerne certains offices) à compter de la date de priorité, **la demande d'examen préliminaire international** doit être présentée à l'administration compétente chargée de l'examen préliminaire international avant l'expiration d'un délai de 19 mois à compter de la date de priorité.

Il appartient exclusivement au déposant de veiller au respect du délai de 19 mois.

Il est à noter que seul un déposant qui est ressortissant d'un État contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international (actuellement, tous les États contractants du PCT sont liés par le chapitre II).

RAPPEL CONCERNANT L'OUVERTURE DE LA PHASE NATIONALE (article 22 ou 39.1))

Si le déposant souhaite que la demande internationale procède en **phase nationale**, il doit, dans le délai de 20 mois ou de 30 mois, ou plus pour ce qui concerne certains offices, accomplir les actes mentionnés dans ces dispositions auprès de chaque office désigné ou élu.

Pour d'autres informations importantes concernant les délais et les actes à accomplir pour l'ouverture de la phase nationale, voir l'annexe du formulaire PCT/IB/301 (Notification de la réception de l'exemplaire original) et le Guide du déposant du PCT, volume II.

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

n° de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé
J. Zahra

n° de téléphone (41-22) 338.91.11

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
15 novembre 2001 (15.11.2001)

PCT

(10) Numéro de publication internationale
WO 01/86601 A1

(51) Classification internationale des brevets[7] : G07F 7/12

(21) Numéro de la demande internationale :
PCT/FR01/01359

(22) Date de dépôt international : 4 mai 2001 (04.05.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/05894 9 mai 2000 (09.05.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **BULL CP8** [FR/FR]; 68, route de Versailles, Boîte postale 45, F-78431 Louveciennes Cedex (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **HAZARD, Michel** [FR/FR]; 27, rue des Harias, F-78124 Mareil sur Mauldre (FR).

(74) Mandataire : **CORLU, Bernard**; Bull CP8, PC62A24, 68, route de Versailles, Boîte postale 45, F-78431 Louveciennes Cedex (FR).

(81) États désignés *(national)* : AU, BR, CA, CN, JP, KR, NO, SG, US.

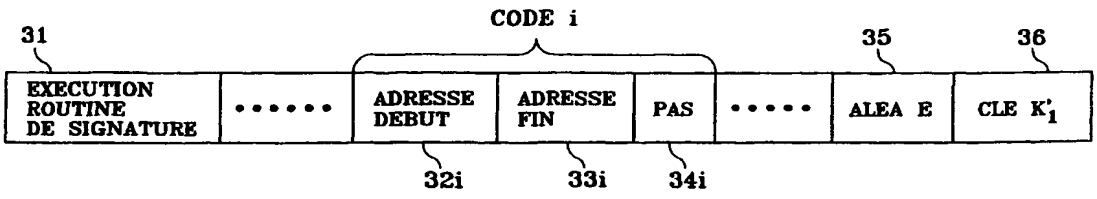
(84) États désignés *(régional)* : brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Publiée :
— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: METHOD FOR AUTHENTICATING A PORTABLE OBJECT, CORRESPONDING PORTABLE OBJECT, AND APPARATUS THEREFOR

(54) Titre : PROCEDE POUR AUTHENTIFIER UN OBJET PORTATIF, OBJET PORTATIF CORRESPONDANT, ET APPAREIL POUR METTRE EN OEUVRE LE PROCEDE



(57) Abstract: The invention concerns a method for authenticating a portable object comprising data processing means and data storage means, the data storage means containing at least a code (i) defining operations capable of being executed by the portable object, and a one-way function. The invention is characterised in that said method comprises a step which consists in sending to the portable object a command (31, 32i-34i, 35, 36) for the latter to execute a calculation of a result by applying to said one-way function at least part of said code (i), said result being used to determine whether the portable object is authentic or not. The invention also concerns the associated portable object and an apparatus designed to co-operate with the portable object.

(57) Abrégé : L'invention concerne un procédé pour authentifier un objet portatif comprenant des moyens de traitement d'information et des moyens de mémorisation d'information, les moyens de mémorisation d'information contenant au moins un code (i) définissant des opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une fonction à sens unique. Selon l'invention, ce procédé comprend l'étape consistant à envoyer à l'objet portatif un ordre (31, 32i-34i, 35, 36) pour que celui-ci exécute un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code (i), ce résultat étant utilisé pour décider si l'objet portatif est authentique ou non. L'invention concerne aussi l'objet portatif associé et un appareil destiné à coopérer avec l'objet portatif.

WO 01/86601 A1

PROCEDE POUR AUTHENTIFIER UN OBJET PORTATIF, OBJET PORTATIF CORRESPONDANT, ET APPAREIL POUR METTRE EN OEUVRE LE PROCEDE

De nombreux domaines d'activité ont aujourd'hui recours à des objets portatifs comportant des moyens de traitement d'information et des moyens de mémorisation d'information, notamment sous la forme de cartes à microprocesseur, pour sécuriser les accès aux services qu'ils offrent. Bien que présentant un niveau de sécurité élevé, ces objets portatifs ne procurent pas une sécurité totale : pour les applications les plus sensibles (porte-monnaie électronique, carte de débit/crédit pour le paiement, télévision à péage), l'authentification de l'objet portatif au moyen de la cryptographie symétrique voire asymétrique s'avère insuffisante. En effet, ce moyen d'authentification repose sur la détention, par les objets portatifs, de clés secrètes. Or, l'expérience prouve que des fraudeurs, très compétents et disposant de moyens importants, arrivent à découvrir des clés secrètes se trouvant pourtant dans des zones mémoire normalement inaccessibles depuis l'extérieur des objets portatifs. Une clé secrète corrompue permet à un fraudeur ou à une organisation frauduleuse de tirer un avantage substantiel en vendant à bas prix des objets portatifs clonés offrant les mêmes services que les objets portatifs authentiques. Le fraudeur réalisera un objet portatif clone de l'objet portatif authentique en réalisant un produit répondant aux fonctions de l'objet portatif authentique, sans prendre en compte tout ce qui limite l'usage de l'objet portatif et tout ce qui concerne la sécurité du produit.

Dans le domaine des cartes à puce, lorsqu'un opérateur de télécommunications, de télévision, ou une institution bancaire a recours à la carte, il met en place une procédure d'acceptation du produit, qui comporte deux volets :

1) l'homologation fonctionnelle du produit, qui garantit la conformité au cahier des charges ;

2) l'évaluation sécuritaire du produit, qui permet de vérifier que les exigences sécuritaires sont satisfaites.

Une fois le produit accepté (sur le plan matériel et logiciel), il n'existe pas de moyen de vérifier qu'une carte a fait l'objet d'une procédure d'acceptation, autre que par l'authentification utilisant une clé secrète, ce qui suppose que cette clé n'a en aucun cas pu être corrompue et ne peut donc qu'être associée à un produit accepté.

L'objet de la présente invention consiste à offrir une solution au problème posé. L'idée de base repose sur le fait qu'une clé secrète ne doit pas être dissociée du produit qui l'exploite, et notamment du code ou programme exécuté par les moyens de traitement d'information de l'objet portatif. Par voie de conséquence, il convient, de façon dynamique, d'authentifier le code avant de faire confiance aux clés. Par « authentification dynamique », on entend une authentification effectuée de façon répétée au cours de la vie de l'objet portatif, plus précisément à l'occasion des différentes sessions dans lesquelles l'objet portatif est utilisé. Par exemple, dans le domaine de la télévision à péage, on authentifiera le code pendant l'émission, à intervalles de temps prédéterminés ; dans le domaine du paiement, on authentifiera le code lors de chaque transaction effectuée dans le cas où le terminal coopérant avec l'objet portatif est en mode « connecté » à une autorité.

L'invention concerne à cet effet un procédé pour authentifier un objet portatif comprenant des moyens de traitement d'information et des moyens de mémorisation d'information, les moyens de mémorisation d'information contenant au moins un code définissant des opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une fonction à sens unique, caractérisé en ce qu'il comprend l'étape consistant à envoyer à l'objet portatif un ordre pour que celui-ci exécute un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code, ce résultat étant utilisé pour décider si l'objet portatif est authentique ou non.

L'invention concerne aussi un procédé pour faire exécuter par un objet portatif une opération sensible, l'objet portatif comprenant des moyens de traitement d'information et des moyens de mémorisation d'information, les moyens de mémorisation d'information contenant au moins un code définissant des opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une fonction à sens unique, caractérisé en ce qu'il comprend l'étape consistant à envoyer à l'objet portatif un ordre pour que celui-ci exécute un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code , ledit résultat intervenant dans la mise en œuvre de ladite opération sensible, cette opération n'étant réalisée avec succès que dans le cas où l'objet portatif est authentique.

L'invention concerne encore un objet portatif comprenant des moyens de traitement d'information et des moyens de mémorisation d'information, les moyens de mémorisation d'information contenant au moins un code définissant des opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une fonction à sens unique, caractérisé en ce qu'il comprend des moyens pour exécuter un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code.

L'invention concerne enfin un appareil comprenant des moyens de traitement d'information et des moyens de mémorisation d'information et agencé pour communiquer avec un objet portatif afin d'authentifier celui-ci, l'objet portatif comprenant des moyens de traitement d'information et des moyens de mémorisation d'information, les moyens de mémorisation d'information de l'objet portatif contenant au moins un code définissant des opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une fonction à sens unique, caractérisé en ce qu'il comprend des moyens pour envoyer à l'objet portatif un ordre pour que celui-ci exécute un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code de l'objet portatif.

D'autres détails et avantages de la présente invention apparaîtront au cours de la description suivante d'un mode d'exécution préféré mais non limitatif, en regard des dessins annexés sur lesquels :

La figure 1 représente un objet portatif coopérant avec un dispositif de traitement d'information ;

La figure 2 est un organigramme d'une procédure de vérification d'une signature calculée par un objet portatif sur un code qu'il détient ;

La figure 3 représente un format de message envoyé à l'objet portatif pour que celui-ci calcule une signature de code ; et

La figure 4 représente une procédure d'authentification d'une carte à puce, conformément aux normes GSM.

La figure 1 représente un dispositif de traitement d'information 1 coopérant avec un objet portatif 7. Le dispositif de traitement d'information comprend de façon connue en soi des moyens de traitement d'information 2 auxquels sont reliés une mémoire non volatile 3, une mémoire RAM 4, des moyens 5 pour coopérer, avec ou sans contact physique, avec l'objet portatif 7, et une interface de transmission 6 permettant au dispositif de traitement d'information de communiquer avec un réseau de communication d'information. Le dispositif de traitement d'information 1 peut en outre être équipé de moyens de stockage tels que des disquettes ou disques amovibles ou non, de moyens de saisie (tels qu'un clavier et/ou un dispositif de pointage du type souris) et de moyens d'affichage, ces différents moyens n'étant pas représentés sur la figure 1.

Le dispositif de traitement d'information peut être constitué par tout appareil informatique installé sur un site privé ou public et apte à fournir des moyens de gestion de l'information ou de délivrance de divers biens ou services, cet appareil étant installé à demeure ou portable. Il peut notamment s'agir aussi d'un appareil dédié aux télécommunications.

Par ailleurs, l'objet portatif 7 porte une puce incluant des moyens de traitement d'information 8, reliés d'un côté à une mémoire non volatile 9 et à une mémoire volatile de travail RAM 10, et reliés d'un autre côté à des moyens 11 pour coopérer avec le dispositif de traitement d'information 1. La mémoire non volatile 9 peut comprendre une partie non modifiable ROM et une partie modifiable EPROM, EEPROM, ou constituée de mémoire RAM du type "flash" ou FRAM (cette dernière étant une mémoire RAM ferromagnétique), c'est-à-dire présentant les caractéristiques d'une mémoire EEPROM avec en outre des temps d'accès identiques à ceux d'une RAM classique.

En tant que puce, on pourra notamment utiliser un microprocesseur autoprogrammable à mémoire non volatile, tel que décrit dans le brevet américain n° 4.382.279 au nom de la Demanderesse. Dans une variante, le microprocesseur de la puce est remplacé - ou tout du moins complété - par des circuits logiques implantés dans une puce à semi-conducteurs. En effet, de tels circuits sont aptes à effectuer des calculs, notamment d'authentification et de signature, grâce à de l'électronique câblée, et non microprogrammée. Ils peuvent notamment être de type ASIC (de l'anglais « Application Specific Integrated Circuit »). Avantageusement, la puce sera conçue sous forme monolithique.

L'objet portatif stocke, dans une zone de sa mémoire non volatile 9 qui est de préférence accessible seulement aux moyens de traitement 8, un code ou programme de fonctionnement incluant l'un ou/et l'autre des programmes suivants :

-un système d'exploitation correspondant à un programme gérant des fonctions de base de l'objet portatif ;

-un programme effectuant une interprétation entre un langage système et un langage de plus haut niveau ;

-un ou plusieurs programmes d'application correspondant à une ou plusieurs applications offertes par l'objet portatif (application carte bancaire,

application porte-monnaie électronique, application contrôle d'accès des personnes, etc...).

De préférence et comme expliqué par la suite, ce code inclura une partie de « programme machine » ou programme écrit avec un langage propre aux moyens de traitement 8.

Ce code peut être stocké dans une zone de mémoire ROM masquée ou dans une zone de mémoire EEPROM de la mémoire non volatile 9, ou encore en partie dans ces deux zones. Le code inclut une routine de signature apte à calculer une signature d'une partie paramétrable du code. Avantageusement, la routine de signature comprend une fonction apte à calculer un condensé de la partie de code : il s'agit par exemple d'un checksum (ou somme de contrôle) ou d'une fonction de hachage telle que MD5 ou SHA, manipulant des bits du code en leur appliquant une fonction mathématique. La routine de signature comprend encore un algorithme de signature apte à signer le condensé de la partie de code : il peut s'agir d'un algorithme symétrique tel que le triple DES (de l'anglais Data Encryption Standard) en mode « MAC » (de l'anglais « Message Authentication Code » ou code d'authentification de message) ou d'un algorithme asymétrique tel que le RSA (des auteurs Rivest, Shamir, et Adleman). L'algorithme de signature utilise une clé secrète K_1 qui, soit est fournie à l'objet portatif au moment de calculer la signature, soit est stockée dans une zone secrète de la mémoire non volatile 9 de l'objet portatif, accessible aux seuls moyens de traitement d'information 8. Un avantage de la première solution est qu'elle permet de modifier dans le temps la clé secrète utilisée. Dans le cas où la clé secrète K_1 est fournie à l'objet portatif, elle l'est de préférence sous forme chiffrée au moyen d'une autre clé K_2 , l'objet portatif détenant, selon le type d'algorithme de chiffrement utilisé, soit cette même clé, soit une clé corrélée à celle-ci, en vue de déchiffrer la clé secrète K_1. De façon connue en soi, le calcul de signature comme celui de chiffrement fait intervenir un aléa fourni à l'objet portatif.

La procédure de communication avec l'objet portatif est représentée sur la figure 2. On suppose que le terminal doit donner à l'objet portatif un ordre d'exécuter une opération sensible déterminée, opération qui requiert au préalable l'authentification du code contenu dans l'objet portatif. A l'étape 21, le terminal 1 transmet à l'objet portatif un ordre de lecture d'informations d'identification de l'objet portatif, stockées en mémoire de l'objet portatif et définissant le type de la puce portée par cet objet et le numéro de version de son système d'exploitation. A l'étape 22, le terminal 1 transmet à l'objet portatif un ordre de calcul de signature pour que celui-ci exécute la routine de signature. Selon une première forme de réalisation dans laquelle le terminal est en mode « connecté » à une autorité via un réseau de communication d'information, c'est-à-dire à un organisme responsable d'une opération sensible à exécuter par l'objet portatif, l'ordre de calcul de signature est émis par l'autorité, le terminal se contentant de transmettre cet ordre à l'objet portatif. Selon une seconde forme de réalisation dans laquelle le terminal est en mode « non connecté » à l'autorité, l'ordre de calcul de signature est émis par le terminal lui-même. Dans tous les cas, l'ordre de calcul de signature prend la forme d'un message dont le format est, selon une forme de réalisation préférée, représenté à la figure 3. Ce message comprend tout d'abord un ordre 31 d'exécuter la routine de signature. Il comprend ensuite, pour chaque code i d'un ensemble de codes 1 à n éventuellement impliqués dans le calcul de signature, une adresse de début 32i désignant l'endroit du code i de l'objet portatif où doit commencer la partie de code à considérer, une adresse de fin 33i où doit se terminer cette partie de code, et un pas 34i définissant, parmi les octets composant le code i, ceux qui seront considérés : par exemple, si ce pas est égal à 7, cela signifie que l'objet portatif considérera, pour son calcul, un octet sur sept, soit le premier octet, puis le huitième, puis le quinzième, etc...Le message comprend ensuite un aléa E (35) qui interviendra dans le calcul de signature puis, seulement dans le cas où la clé secrète de signature n'est pas stockée dans l'objet portatif, cette clé secrète de signature K_1' (36), chiffrée. De

préférence, les valeurs suivantes changent à chaque procédure de vérification de signature : adresses de début, adresses de fin, pas, aléa E ; on notera cependant qu'une sécurité satisfaisante est déjà obtenue en ne faisant varier que l'une de ces valeurs.

On notera que, dans le cas où l'un des codes impliqués dans le calcul de signature est écrit en un langage évolué et non dans le langage machine propre aux moyens de traitement 8 de l'objet portatif, ce qui est peut être par exemple le cas pour une application bancaire, les adresses de début 32i et de fin 33i sont remplacées par un identifiant général de ce code.

De préférence, lorsque la clé secrète de signature K_1' est présente dans le message, le message inclura en outre un checksum ou une signature du message. A réception du message par l'objet portatif, celui-ci recalculera le checksum ou la signature, ce qui lui permettra :

-de s'assurer de l'origine du message ;

-de vérifier qu'il n'y a pas eu d'incident de transmission.

A l'étape 23, l'objet portatif exécute le calcul de signature. Dans le cas où il a reçu la clé secrète chiffrée K_1', il déchiffre cette clé au moyen d'une clé de déchiffrement. Il calcule un condensé des parties de code à considérer, puis il signe ce condensé avec la clé secrète K_1 en faisant intervenir l'aléa E. A l'étape 24, l'objet portatif transmet la signature ainsi calculée au terminal 1.

Dans le cas où le terminal fonctionne en mode « non connecté », il vérifie lui-même la signature (étape 25). De préférence, le terminal ne connaît ni le (les) code(s) authentique(s), ni la clé K_1 , laquelle est supposée être détenue par l'objet portatif. L'autorité fournit au terminal un message conforme à la figure 3, à l'exception de la clé K_1', et une signature précalculée correspondant à ce message particulier. Le terminal enverra à l'objet portatif ledit message et, à réception de la signature en provenance de l'objet portatif, vérifiera celle-ci par comparaison avec sa signature précalculée. Si la comparaison aboutit positivement, le ou les codes de l'objet portatif sont authentifiés et le terminal donne l'ordre à l'objet portatif

d'exécuter l'opération sensible précitée (étape 26). Dans la négative, le terminal met au rebut ou rejette l'objet portatif (étape 27).

Dans le cas où le terminal fonctionne en mode « connecté » à une autorité, c'est l'autorité qui émet le message de la figure 3, lequel sera retransmis par le terminal à l'objet portatif. L'autorité stocke à cet effet dans une mémoire le ou les codes de l'objet portatif et, soit la clé secrète K_1 , soit une clé corrélée à celle-ci . elle stocke aussi en mémoire les autres paramètres contenus dans le message de la figure 3. L'autorité peut, soit précalculer ou recalculer la signature en utilisant l'algorithme de signature et la clé secrète K_1 et la comparer avec la signature reçue de l'objet portatif (étape 25) via le terminal, soit utiliser la signature reçue de l'objet portatif pour recalculer le condensé des codes de l'objet portatif en utilisant un algorithme inverse de l'algorithme de signature et, selon l'algorithme utilisé, soit la clé secrète K_1 , soit ladite clé corrélée à celle-ci ; l'autorité compare ensuite le condensé ainsi recalculé avec un condensé des codes qu'elle détient en mémoire. C'est aussi l'autorité qui déclenchera l'exécution de l'opération sensible (étape 26, figure 2) ou la mise au rebut ou le rejet de l'objet portatif (étape 27), le terminal servant seulement d'intermédiaire. On notera que la procédure en mode « terminal connecté à l'autorité » est plus fiable que celle en mode « terminal non connecté à l'autorité ».

En variante, la signature calculée par l'objet portatif n'est pas envoyée à l'extérieur juste après son calcul, mais est conservée dans l'objet portatif et mise à disposition du monde extérieur de façon qu'elle puisse être lue ultérieurement.

En cas de fraude, une clé a généralement pu être découverte par le fraudeur, permettant à celui-ci d'émettre une quantité importante d'objets portatifs clones, contenant cette clé. Ces objets portatifs contiennent un code réduit assurant seulement les fonctionnalités indispensables pour mettre en oeuvre une application que vise à utiliser le fraudeur, à l'exclusion notamment des fonctions sécuritaires : ce code est donc différent du ou des codes d'un objet portatif authentique. La procédure de la figure 2 produira

une signature non conforme à la signature authentique, ce qui permettra d'écarter tous ces objets portatifs.

Si le ou les codes des objets portatifs authentiques contiennent un code machine, l'authentification est encore plus fiable. En effet, supposons que le fraudeur ait pu arriver, à l'aide de moyens très perfectionnés, à obtenir le code contenu dans un objet portatif authentique : il doit alors, pour que les objets portatifs clones puissent se faire authentifier, mettre ce code dans chaque objet portatif clone sous forme de table de données, en plus du code non authentique contenu dans les objets portatifs clones, afin que le calcul d'authentification porte sur le code authentique. En effet, l'objet portatif clone utilisera le plus souvent des moyens de traitement différents de ceux de l'objet portatif authentique, c'est-à-dire utilisant un code machine écrit dans un langage différent, ce code machine ne permettant pas d'aboutir à une authentification réussie. La nécessité, pour le fraudeur, de stocker dans chaque objet portatif, outre son propre code, celui d'un objet portatif authentique, constitue un handicap important qui est de nature à décourager la fraude.

Un premier exemple d'opération sensible à sécuriser est le suivant : il s'agit d'une opération de personnalisation d'objets portatifs constitués par des cartes à puce. Cette opération, effectuée chez une autorité, consiste à stocker, dans une zone secrète de la mémoire non volatile des cartes, des clés « émetteur » appartenant à l'organisme émetteur des cartes considérées, ainsi que des clés « applicatives », permettant aux cartes d'avoir accès à différentes applications. Selon l'invention, le stockage de ces clés en carte ne s'effectuera que si la procédure de vérification de la figure 2 aboutit positivement.

Un deuxième exemple d'opération sensible à sécuriser est celui de la télévision à péage. Ce domaine est l'objet de fraude permanente affectant un appareil décodeur d'image utilisé dans cette application, et plus récemment les cartes utilisées en association avec cet appareil. Les cartes clones

contiennent un code réduit permettant de délivrer une clé de désembrouillage de l'image de télévision.

Dans un mode de fonctionnement classique, chaque carte de télévision reçoit périodiquement des messages dits « de contrôle », qui contiennent des données de contrôle (date, droits, etc..., et une clé de désembrouillage chiffrée) ; l'ensemble de chaque message est signé. La carte vérifie la signature, puis déchiffre la clé de désembrouillage. Selon l'invention, on ne délivre pas à la carte la clé de désembrouillage mais un message du type de celui de la figure 3, lui demandant d'effectuer un calcul sur une partie du ou des code(s) de la carte, calcul dont le résultat constitue la clé de désembrouillage si et seulement si le code de la carte est authentique. On constate donc que, dans cet exemple, la carte ne transmet pas de résultat de calcul à une autorité pour son authentification, l'authentification étant implicite et se manifestant par le désembrouillage effectif de l'image de télévision.

Un troisième exemple d'opération sensible à sécuriser concerne le domaine des cartes de débit/crédit. Avant que le terminal n'autorise une opération de débit/crédit de la carte, il déclenchera la procédure de la figure 2, de préférence en mode « connecté » à une autorité bancaire.

Avantageusement, l'organisme émetteur des objets portatifs communiquera aux organismes utilisateurs de ces objets portatifs, comme moyen de vérification de l'authenticité de ces objets portatifs à l'occasion de leur personnalisation et avant leur diffusion à des usagers individuels, au moins un objet portatif de référence dûment authentifié par l'organisme émetteur. L'authentification d'un objet portatif consistera à faire calculer une signature du code à la fois dans cet objet portatif et dans l'objet portatif de référence, la comparaison des deux résultats permettant de conclure sur l'authenticité de l'objet portatif à vérifier. La sélection, par l'organisme utilisateur, de l'objet portatif de référence approprié parmi un ensemble d'objets portatifs de référence éventuellement détenus par cet organisme s'effectue au moyen des informations d'identification précitées (étape 21 de

la figure 2). Ce procédé a l'avantage, pour l'organisme émetteur des objets portatifs, de ne pas communiquer aux organismes utilisateurs le contenu du (des) code(s) des objets portatifs, c'est-à-dire son savoir-faire. Il est donc plus sécuritaire pour lui.

Avantageusement, la procédure de la figure 2 sera précédée d'une opération d'authentification de la personne ou de l'organisme mettant en oeuvre cette procédure, selon des moyens connus basés sur la détention, par cette personne ou cet organisme, d'un PIN (de l'anglais Personal Identification Number) ou mieux d'une clé.

Selon une variante de réalisation de l'invention moins avantageuse, le procédé d'authentification de l'objet portatif consiste à vérifier la signature de d'une partie fixe du code contenu dans cet objet portatif, éventuellement de l'ensemble du code, et non d'une partie de celui-ci variable lors de chaque procédure d'authentification.

Selon une autre variante de réalisation de l'invention moins avantageuse, le procédé d'authentification de l'objet portatif n'inclut pas l'opération consistant à condenser le code avant sa signature.

On notera que, si le code est stocké dans l'objet portatif en laissant des espaces mémoire vides, il sera avantageux de combler ces espaces avec un code fictif qui ne remplira aucune fonction mais rendra le code plus volumineux, ce qui gênera d'autant plus le fraudeur dans sa tentative de recopier ce code sur des objets portatifs clones. Par « code fictif », on entend un code écrit dans un langage réel mais qui ne sera jamais utilisé, c'est-à-dire jamais exécuté. Par opposition, le code effectivement utilisé sera appelé « code réel ».

Il existe le risque qu'un fraudeur arrive à identifier le code manipulé lors de l'opération de signature selon l'invention, en observant le bruit généré par l'objet portatif. Selon l'invention, on limite ce risque en ne signant du code réel que de temps en temps, notamment à l'occasion d'opérations jugées cruciales du point de vue sécuritaire. Une telle opération est par exemple celle de personnalisation de l'objet portatif, dans laquelle des

moyens applicatifs sont insérés dans l'objet portatif, notamment des clés et des codes applicatifs. Par contre, lors d'opérations courantes moins sensibles et plus répétitives, il sera demandé à l'objet portatif de signer du code fictif.

Il serait utile d'empêcher un fraudeur de se faire passer pour une autorité habilitée en interrogeant l'objet portatif selon la procédure de la figure 2, et en répétant cette opération un grand nombre de fois, de façon à observer les informations circulant dans l'objet portatif. A cet effet, et selon un perfectionnement de l'invention, l'objet portatif est agencé pour limiter le nombre d'appels à la routine de signature à un nombre prédéterminé.

Une application de l'invention au domaine GSM (de l'anglais « Global System for Mobile communications ») va maintenant être présentée. La figure 4 rappelle le procédé défini par les normes GSM, d'authentification par un serveur d'authentification 41, de la carte à puce 42 équipant un mobile GSM 43. On rappelle que le mobile 43 dialogue avec le serveur 41 via une base station 44. Le procédé comprend une première étape selon laquelle la carte envoie au serveur un identifiant IMSI définissant l'identité d'un abonné porteur du mobile, ainsi que l'identité de la carte, donc du code qui y est contenu. En réponse, le serveur envoie à la carte un aléa. A partir de cet aléa, la carte exécute une commande connue sous le nom de « RUN GSM ALGO » calculant une valeur d'authentification nommée SRES' et une clé K_C à partir d'une clé KI propre à la carte. De son côté, le serveur calcule une valeur d'authentification de référence SRES'. La carte envoie ensuite sa valeur d'authentification SRES au serveur, lequel la compare à sa valeur d'authentification de référence SRES' afin de déterminer si la carte est authentique ou non.

Selon l'invention, le procédé d'authentification ci-dessus est modifié comme suit : au lieu d'envoyer à la carte un aléa classique constitué par un nombre défini par le serveur, celui-ci lui envoie le message de la figure 3. A

réception, la carte calcule une signature de code selon l'étape 23 de la figure 2, basée sur une clé de signature déterminée K_1 . Ensuite, la carte calcule la valeur d'authentification SRES conformément aux normes GSM, mais en utilisant, en tant qu'aléa, le résultat de la signature de code au lieu de l'aléa habituellement fourni par le serveur. De préférence, le procédé selon l'invention ne sera pas mis en œuvre lors de chaque session entre le mobile et le serveur mais seulement de temps en temps, de façon à réduire le risque qu'un fraudeur arrive à identifier le code manipulé lors de l'opération de signature selon l'invention, en observant le bruit généré par la carte.

Dans ce qui précède, on a décrit une authentification du code de l'objet portatif par calcul de signature. En variante, on peut effectuer cette authentification au moyen d'un calcul de chiffrement/déchiffrement, comme cela est connu en soi. Dans le cas d'un algorithme symétrique, l'objet portatif calculera un chiffré de son code avec une clé secrète et l'enverra au terminal ou à l'autorité qui effectuera l'authentification par chiffrement ou déchiffrement. Dans le cas d'un algorithme asymétrique, l'objet portatif calculera un chiffré de son code avec une clé publique et l'enverra au terminal ou à l'autorité qui effectuera l'authentification par chiffrement ou déchiffrement. Par ailleurs, on a présenté dans ce qui précède un calcul d'authentification qui mettait en œuvre un algorithme cryptographique manipulant une ou plusieurs clés, dont l'une est secrète. Un tel algorithme, comme le DES ou RSA précités, est dit « trap-door one way », les termes « one way » signifiant que la fonction utilisée est à sens unique, et les termes « trap-door » signifiant qu'il existe un secret. On rappelle qu'une fonction à sens unique est une fonction qui peut être calculée dans un sens sans information particulière, mais qui ne peut pas être calculée de façon inverse, sauf éventuellement si l'on connaît certains paramètres. Dans le cas du DES et du RSA, ces paramètres consistent dans la clé secrète. Selon l'invention, l'utilisation d'une fonction « trap-door » est intéressante en ce qu'elle apporte une sécurité supplémentaire basée sur la clé secrète, mais elle n'est pas nécessaire : il suffit en effet, pour réaliser l'opération d'authentification du

code de l'objet portatif, d'effectuer un calcul sur ce code avec toute fonction à sens unique, en l'absence de toute manipulation de clé. Une fonction à sens unique est notamment une fonction de hachage telle que MD5 ou SHA citées précédemment.

REVENDICATIONS

1. Procédé pour authentifier un objet portatif (7) comprenant des moyens de traitement d'information (8) et des moyens de mémorisation d'information (9,10), les moyens de mémorisation d'information contenant au moins un code (i) définissant des opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une fonction à sens unique, caractérisé en ce qu'il comprend l'étape consistant à envoyer à l'objet portatif un ordre (31,32i-34i, 35,36) pour que celui-ci exécute un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code (i), ce résultat étant utilisé pour décider si l'objet portatif est authentique ou non.

2. Procédé selon la revendication 1, dans lequel ledit résultat intervient dans la mise en œuvre d'une opération déterminée, cette opération n'étant réalisée avec succès que dans le cas où l'objet portatif (7) est authentique.

3. Procédé selon la revendication 2, dans lequel ladite opération déterminée comprend un déchiffrement d'information, ledit résultat permettant de produire une clé de déchiffrement associée.

4. Procédé selon la revendication 1, dans lequel ladite partie de code (i) utilisée dans le calcul comprend une partie de code machine.

5. Procédé selon la revendication 1, dans lequel l'objet portatif (7) contient un code dit « réel » définissant des opérations destinées à être exécutées par l'objet portatif, et un code dit « fictif » définissant des opérations non destinées à être exécutées par l'objet portatif, ladite partie de code utilisée dans le calcul comprenant une partie de code fictif.

6. Procédé selon la revendication 1, dans lequel ledit ordre (31,32i-34i, 35,36) est envoyé de façon répétitive à l'objet portatif au cours de sa vie, avant l'exécution, par celui-ci, desdites opérations.

7. Procédé selon la revendication 1, dans lequel ladite partie de code (i) utilisée dans le calcul est définie par une adresse de début (32i) et une adresse de fin (33i) dans les moyens de mémorisation d'information, lesdites adresses étant envoyées à l'objet portatif.

8. Procédé selon la revendication 1, dans lequel ledit code (i) comprend un ensemble de mots binaires, ladite partie de code utilisée dans le calcul étant définie par un sous-ensemble de mots binaires comprenant les mots binaires répartis dans les moyens de mémorisation d'information selon un pas déterminé (34i), ledit pas étant envoyé à l'objet portatif.

9. Procédé pour faire exécuter par un objet portatif (7) une opération sensible, l'objet portatif comprenant des moyens de traitement d'information (8) et des moyens de mémorisation d'information (9,10), les moyens de mémorisation d'information contenant au moins un code (i) définissant des opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une fonction à sens unique, caractérisé en ce qu'il comprend l'étape consistant à envoyer à l'objet portatif un ordre (31,32i-34i, 35,36) pour que celui-ci exécute un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code (i), ledit résultat intervenant dans la mise en œuvre de ladite opération sensible, cette opération n'étant réalisée avec succès que dans le cas où l'objet portatif (7) est authentique.

10. Procédé selon la revendication 9, dans lequel ladite partie de code (i) utilisée dans le calcul comprend une partie de code machine.

11. Procédé selon la revendication 9, dans lequel l'objet portatif contient un code dit « réel » définissant des opérations destinées à être exécutées par l'objet portatif, et un code dit « fictif » définissant des opérations non destinées à être exécutées par l'objet portatif, ladite partie de code utilisée dans le calcul comprenant une partie de code fictif.

12. Objet portatif comprenant des moyens de traitement d'information (8) et des moyens de mémorisation d'information (9,10), les moyens de mémorisation d'information contenant au moins un code (i) définissant des opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une fonction à sens unique, caractérisé en ce qu'il comprend des moyens pour exécuter un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code.

13. Objet portatif selon la revendication 12, dans lequel ladite partie de code (i) utilisée dans le calcul comprend une partie de code machine.

14. Appareil (1) comprenant des moyens de traitement d'information (2) et des moyens de mémorisation d'information (3,4) et agencé pour communiquer avec un objet portatif (7) afin d'authentifier celui-ci, l'objet portatif comprenant des moyens de traitement d'information (8) et des moyens de mémorisation d'information (9,10), les moyens de mémorisation d'information de l'objet portatif contenant au moins un code (i) définissant des opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une fonction à sens unique, caractérisé en ce qu'il comprend des moyens pour envoyer à l'objet portatif un ordre (31,32i-34i, 35,36) pour que celui-ci exécute un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code (i) de l'objet portatif.

15. Appareil selon la revendication 14, dans lequel ladite partie de code (i) utilisée dans le calcul comprend une partie de code machine.

1/2

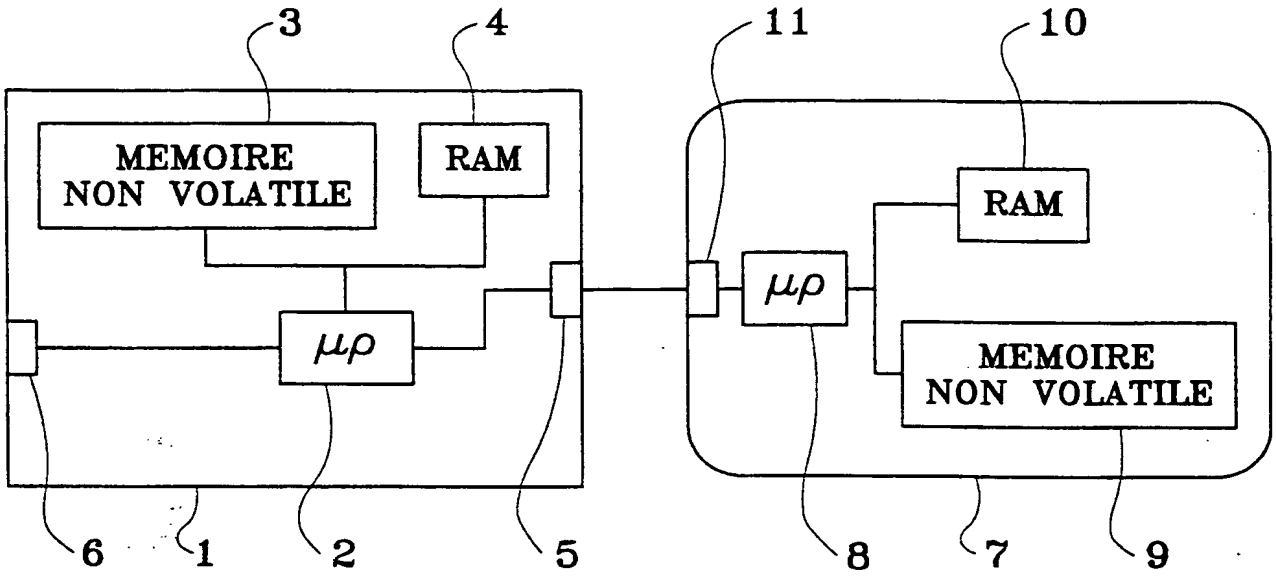

3
4
11
10
MEMOIRE NON VOLATILE
RAM
RAM
μp
μp
MEMOIRE NON VOLATILE
6
1
2
5
8
7
9

FIG.1

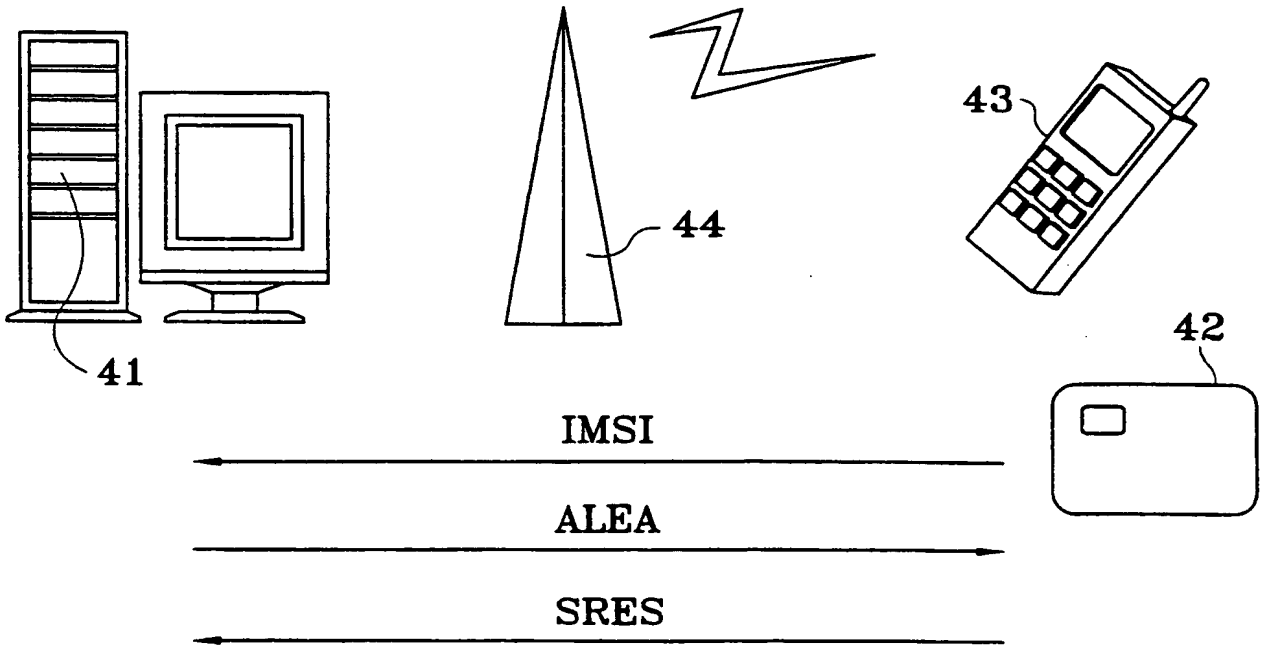

43
44
42
41
IMSI
ALEA
SRES

FIG.4

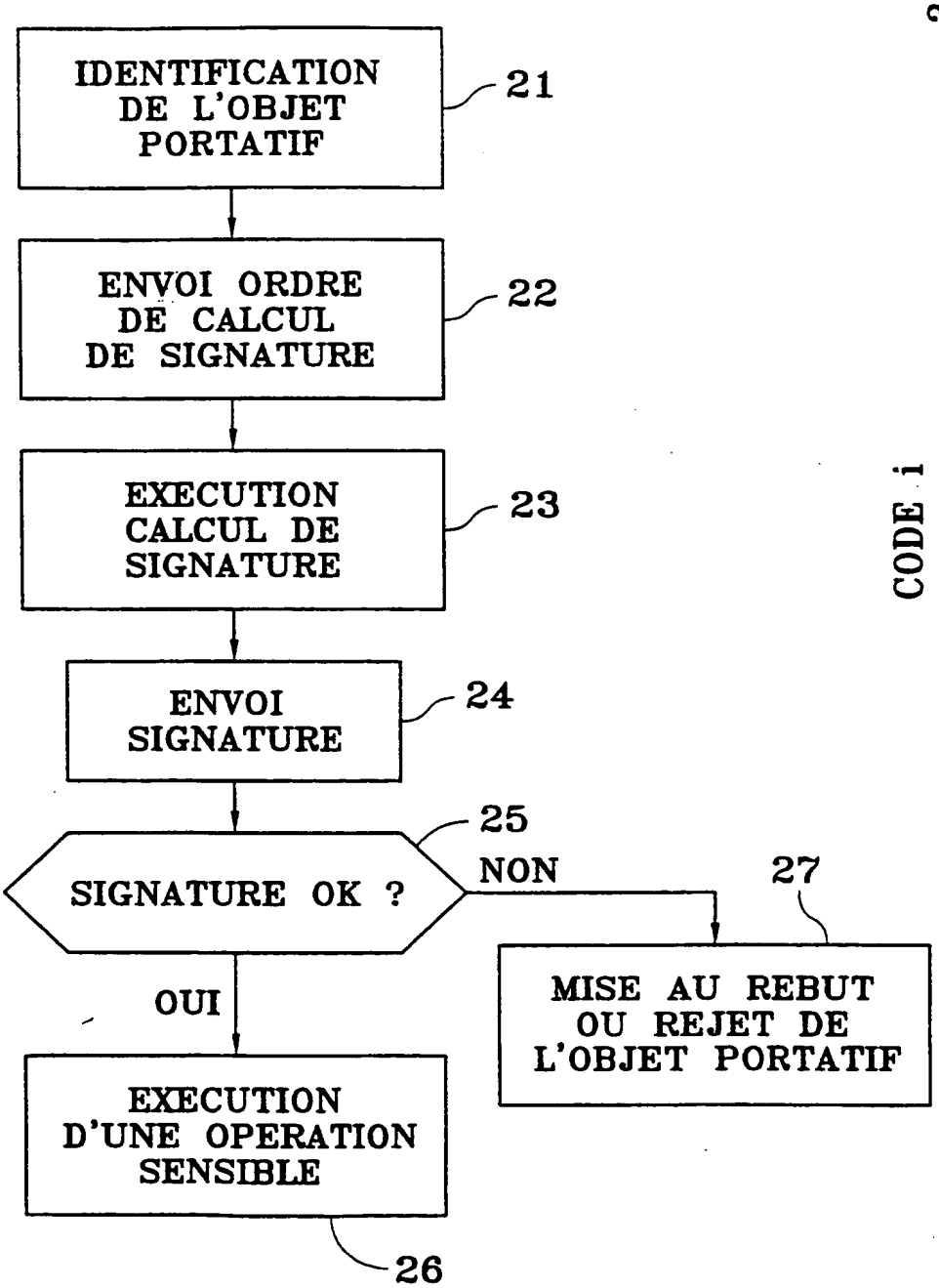

IDENTIFICATION DE L'OBJET PORTATIF
21
ENVOI ORDRE DE CALCUL DE SIGNATURE
22
EXECUTION CALCUL DE SIGNATURE
23
ENVOI SIGNATURE
24
SIGNATURE OK ?
25
NON
27
MISE AU REBUT OU REJET DE L'OBJET PORTATIF
OUI
EXECUTION D'UNE OPERATION SENSIBLE
26

FIG.2

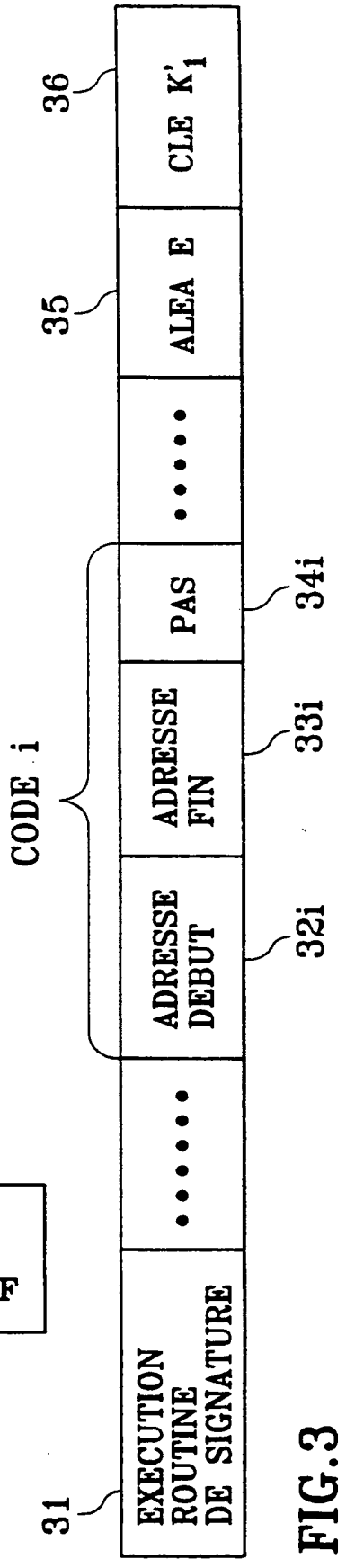

36
CLE K'1
35
ALEA E
PAS
34i
ADRESSE FIN
33i
ADRESSE DEBUT
32i
CODE i
EXECUTION ROUTINE DE SIGNATURE
31

FIG.3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/01359

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 281 058 A (SIEMENS) 7 September 1988 (1988-09-07) the whole document	1,2,6-9, 12,14
Y	FR 2 757 979 A (GEMPLUS) 3 July 1998 (1998-07-03) abstract; claims; figures	1,2,6-9, 12,14
A	EP 0 926 624 A (OKI ELECTRIC INDUSTRY) 30 June 1999 (1999-06-30)	
A	EP 0 475 837 A (GEMPLUS CARD INTERNATIONAL) 18 March 1992 (1992-03-18)	
A	EP 0 531 194 A (GEMPLUS CARD INTERNATIONAL) 10 March 1993 (1993-03-10)	

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 July 2001	30/07/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/01359

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98 37663 A (POSTGIROT BANK) 27 August 1998 (1998-08-27)	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 01/01359

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0281058 A	07-09-1988	AT 85444 T	15-02-1993
		DE 3877984 A	18-03-1993
		ES 2041712 T	01-12-1993
		JP 63229541 A	26-09-1988
		US 4786790 A	22-11-1988
FR 2757979 A	03-07-1998	AU 723007 B	17-08-2000
		AU 5767898 A	31-07-1998
		EP 0974131 A	26-01-2000
		WO 9829843 A	09-07-1998
EP 0926624 A	30-06-1999	JP 11191149 A	13-07-1999
EP 0475837 A	18-03-1992	FR 2666671 A	13-03-1992
		CA 2051365 A,C	13-03-1992
		DE 69100256 D	16-09-1993
		DE 69100256 T	17-02-1994
		JP 4257031 A	11-09-1992
		JP 7056629 B	14-06-1995
		US 5191608 A	02-03-1993
EP 0531194 A	10-03-1993	FR 2680892 A	05-03-1993
		JP 5217033 A	27-08-1993
		US 5343530 A	30-08-1994
WO 9837663 A	27-08-1998	SE 508844 C	09-11-1998
		AU 725952 B	26-10-2000
		AU 6126898 A	09-09-1998
		BR 9807372 A	14-03-2000
		CN 1248367 T	22-03-2000
		EP 0962071 A	08-12-1999
		NO 993939 A	19-10-1999
		SE 9700587 A	20-08-1998

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 01/01359

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/12

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultee (systeme de classification suivi des symboles de classement)
CIB 7 G07F G06F

Documentation consultee autre que la documentation minimale dans la mesure ou ces documents relevent des domaines sur lesquels a porte la recherche

Base de donnees electronique consultee au cours de la recherche internationale (nom de la base de donnees, et si realisable, termes de recherche utilises)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Categorie °	Identification des documents cites, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visees
Y	EP 0 281 058 A (SIEMENS) 7 septembre 1988 (1988-09-07) le document en entier	1,2,6-9, 12,14
Y	FR 2 757 979 A (GEMPLUS) 3 juillet 1998 (1998-07-03) abrégé; revendications; figures	1,2,6-9, 12,14
A	EP 0 926 624 A (OKI ELECTRIC INDUSTRY) 30 juin 1999 (1999-06-30)	
A	EP 0 475 837 A (GEMPLUS CARD INTERNATIONAL) 18 mars 1992 (1992-03-18)	
A	EP 0 531 194 A (GEMPLUS CARD INTERNATIONAL) 10 mars 1993 (1993-03-10)	

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Categories speciales de documents cites:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
20 juillet 2001	30/07/2001

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 01/01359

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visees
A	WO 98 37663 A (POSTGIROT BANK) 27 août 1998 (1998-08-27) -----	

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements rela. aux membres de familles de brevets

Demande internationale No
PCT/FR 01/01359

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 0281058	A	07-09-1988	AT	85444 T	15-02-1993
			DE	3877984 A	18-03-1993
			ES	2041712 T	01-12-1993
			JP	63229541 A	26-09-1988
			US	4786790 A	22-11-1988
FR 2757979	A	03-07-1998	AU	723007 B	17-08-2000
			AU	5767898 A	31-07-1998
			EP	0974131 A	26-01-2000
			WO	9829843 A	09-07-1998
EP 0926624	A	30-06-1999	JP	11191149 A	13-07-1999
EP 0475837	A	18-03-1992	FR	2666671 A	13-03-1992
			CA	2051365 A,C	13-03-1992
			DE	69100256 D	16-09-1993
			DE	69100256 T	17-02-1994
			JP	4257031 A	11-09-1992
			JP	7056629 B	14-06-1995
			US	5191608 A	02-03-1993
EP 0531194	A	10-03-1993	FR	2680892 A	05-03-1993
			JP	5217033 A	27-08-1993
			US	5343530 A	30-08-1994
WO 9837663	A	27-08-1998	SE	508844 C	09-11-1998
			AU	725952 B	26-10-2000
			AU	6126898 A	09-09-1998
			BR	9807372 A	14-03-2000
			CN	1248367 T	22-03-2000
			EP	0962071 A	08-12-1999
			NO	993939 A	19-10-1999
			SE	9700587 A	20-08-1998